Navajo County

Mobile Device Procedure	Created: 4/24/2015
Section of: Corporate Security Procedures	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 5

1.0 Overview

Generally speaking, a more mobile workforce is a more flexible and productive workforce. For this reason, business use of mobile devices is growing. However, as these devices become vital tools to the workforce, more and more sensitive data is stored on them, and thus the risk associated with their use is growing. Special consideration must be given to the security of mobile devices.

2.0 Purpose

The purpose of this procedure is to specify Navajo County standards for the use and security of mobile devices.

3.0 Scope

This procedure applies to Navajo County data as it relates to mobile devices that are capable of storing such data, including, but not limited to, laptops, notebooks, PDAs, smartphones, and USB drives. Since the procedure covers the data itself, ownership of the mobile device is irrelevant. This procedure covers any mobile device capable of coming into contact with County data.

4.0 Procedure

4.1 Physical Security

By nature, a mobile device is more susceptible to loss or theft than a non-mobile system. Navajo County should carefully consider the physical security of its mobile devices and take appropriate protective measures, including the following:

• Laptop locks and cables can be used to secure laptops when in the office or other fixed locations.

• Mobile devices should be kept out of sight when not in use.

• Care should be given when using or transporting mobile devices in busy areas.

• As a general rule, mobile devices should not be stored in cars. If the situation leaves no other viable alternatives, the device should be stored in the trunk, with the interior trunk

release locked; or in a lockable compartment such as a glove box.

• Each Department at Navajo County should evaluate the data that will be stored on mobile devices and consider remote wipe/remote delete technology. This technology allows a user or administrator to make the data on the mobile device unrecoverable.

• Navajo County IT will continue to monitor the market for physical security products for mobile devices, as it is constantly evolving.

4.2 Data Security

If a mobile device is lost or stolen, the data security controls that were implemented on the device are the last line of defense for protecting Navajo County data. The following sections specify the County's requirements for data security as it relates to mobile devices.

4.2.1 Laptops

Use of encryption is not required but it is encouraged if data stored on the device is classified as ACJIS, AJIN, HIPPA, Personally Identifiable Information (PII) or Confidential. Laptops require a username and password or biometrics for login.

4.2.2 PDAs/Smartphones

Use of encryption is not required on PDAs/smartphones but it is encouraged. Smartphones must require at least a four digit PIN/Password or biometrics for login to the device if Navajo County email is installed. There will be a forced push of this requirement by the IT department. If the PIN/Password is entered incorrectly 10 times the device will be reset to factory settings.

4.2.3 Mobile Storage Media

This section covers any USB drive, flash drive, memory stick or other personal data storage media. Storage of County data on such devices is discouraged, but their use is permitted with Department approval. When the USB drive is retired from use it should be wiped and formatted of all County data.

4.2.4 Portable Media Players

Portable media players are gaining in popularity and increasingly being connected to machines that store County data. The County encourages the use of technology, thus users can store County data on personal media players as is necessary.

4.2.5 Other Mobile Devices

Unless specifically addressed by this procedure, storing County data on other mobile devices, or connecting such devices to County systems, is expressly prohibited. Questions or requests for clarification on what is and is not covered should be directed to the IT Director.

4.3 Connecting to Unsecured Networks

Users must not connect to any outside network without a secure, up-to-date software firewall configured on the mobile computer. Examples of unsecured networks would typically, but not always, relate to Internet access, such as access provided from a home network, access provided by a hotel, an open or for-pay wireless hotspot, a convention network, or any other network not under direct control of the Navajo County. Please contact the IT Department if you are concerned that your mobile device is not up-to-date.

4.4 General Guidelines

The following guidelines apply to the use of mobile devices:

• Loss, Theft, or other security incident related to a County-provided mobile device must be reported promptly to the IT Department.

• When Data stored on mobile devices is removed it must be securely disposed of properly. Please contact the IT Department.

• Users should take precautions when storing County data on non-County-provided mobile devices.

4.5 Audits

The County IT Department may conduct periodic reviews to ensure procedure compliance. A sampling of mobile devices could be taken and audited against this procedure on a periodic basis.

4.6 Applicability of Other Procedures

This document is part of Navajo County's cohesive set of security procedures. Other procedures may apply to the topics covered in this document and as such the applicable procedures should be reviewed as needed.

5.0 Enforcement

This procedure will be enforced by the IT Director and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of County property (physical or intellectual) are suspected, Navajo County may report such activities to the applicable authorities.

6.0 Definitions

Encryption – The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Mobile Devices – A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

Mobile Storage Media – A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

Password – A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.

Biometrics – The process by which a person's unique physical and other traits are detected and recorded by an electronic device or system as a means of confirming identity.

PDA – stands for Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar, and notes.

PIN – A sequence of numbers that is used to authenticate a user to a PDA or smartphone.

Portable Media Player – A mobile entertainment device used to play audio and video files. Examples are mp3 players and video players.

Smartphone – A mobile telephone that offers additional applications, such as PDA functions and email.

7.0 Revision History

Revision 1.0, 4/24/2015

Navajo County

Revision 1.5, 9/23/2015
Revision 1.8, 06/08/2016